

## REMARKS

Claims 3-11 remain pending in this application. No claims have been amended, added or cancelled herein.

In the final Office Action mailed 04/4/2008, the Examiner rejects claims 8-11 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2002/0106202 to Hunter in view of U.S. Patent Publication No. 2003/0008662 to Stern et al. ("Stern"), in further view of U.S. Patent No. 7,079,656 to Menzel et al. ("Menzel"). Applicants respectfully traverse these rejections.

### Claim Rejections – 35 U.S.C. § 103(a)

Claims 8-11 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2002/0106202 to Hunter in view of U.S. Patent Publication No. 2003/0008662 to Stern et al. ("Stern"), in further view of U.S. Patent No. 7,079,656 to Menzel et al. ("Menzel"). Applicants respectfully traverse these rejections.

Exemplary embodiments of Applicants' claimed invention provide methods and devices comprising unique combinations of method steps and features, respectively, including, *inter alia*, a method for releasing a locked state of a camera in a portable terminal by means of a cipher apparatus connected to the portable terminal, the portable terminal includes the camera for photographing an image, a memory for storing secret codes, an image processor for processing the photographed image, and a display unit for displaying the processed image, the method comprising the steps of: (1) the cipher apparatus receiving information of the portable terminal, and obtaining a secret code for the locked state of the camera from a database; (2) the cipher apparatus transmitting enciphered data obtained from the secret code; (3) the portable

terminal receiving and deciphering the enciphered data, and comparing the secret code received from the cipher apparatus with one of the secret codes stored in the memory; and (4) enabling the camera to operate when the secret code matches said one of the secret codes stored in the memory.

Neither Hunter, Stern et al. nor Menzel et al., alone or in combination, discloses, teaches or suggests such unique combinations of features or method steps.

The Examiner asserts that arguments in the previous amendment were not recited in claims 8-11, such as the cipher apparatus storing and displaying the secret code and telephone number of the portable terminal. The Examiner further asserts that although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims.

With respect to independent claim 8, the combination of Hunter, Stern and Menzel does not disclose or teach a cipher apparatus that obtains a secret code for the locked state of the camera from a database, the cipher apparatus transmitting enciphered data obtained from the secret code, a portable terminal that compares the secret code received from the cipher apparatus with one of the secret codes stored in the memory, and enabling the camera to operate when the secret code matches said one of the secret codes stored in the memory.

Hunter discloses portable cameras that receive signals from transmitters that cause one or more functions of the camera to be controlled accordingly. In response to receipt of the transmitted signal, the camera may be arranged to disable one or more functions of the camera. The camera is arranged to be enabled or active in a limited area or number of locations. *See* paragraph [0013]. Hunter further discloses a unit 100 housed within a portable camera and includes a smart card reader 102 for receiving a smart card 104 and a disable module 106 arranged to disable one or more of the functions of the portable camera, in accordance with data stored on the smart card 104.

However, there is nothing in Hunter that discloses or teaches a **cipher apparatus** that receives information of the portable terminal, **obtains a secret code** for the locked state of the camera from a database, and **transmits enciphered data**

**obtained from the secret code.** Nowhere does Hunter teach or suggest that the portable camera receives and deciphers **enciphered data and compares a secret code received from a cipher apparatus with one of the secret codes stored in the memory of the camera.** There is also nothing in Hunter that discloses or teaches that the camera is enabled **when a secret code matches one of the secret codes stored in the memory.** The data on the smart card of Hunter does not comprise a secret code.

The Examiner acknowledges that Hunter does not teach enciphering the data, receiving information of the portable terminal, and obtaining a secret code for the locked state of the camera from a database. To cure the deficiencies of Hunter, the Examiner relies on Stern for teaching a method for receiving information regarding the mobile user device and finding a policy based on the device and location information in a database which is sent to the mobile devices by referencing Figure 3, blocks 304 and 306, Figure 4, blocks 800 and 900, paragraphs [0053]-[0056], [0058] and [0059]. According to the Examiner, it would have been obvious to one of ordinary skill in the art at the time the invention was made to receive information regarding the mobile device and obtain a policy for the camera from a database, since Stern discloses in paragraph [0006] that it allows the system to establish a policy based on the location and user device information thereby allowing high priority users to receive phone calls in dire situations, such as a doctor receiving emergency phone calls.

Stern discloses a mobile user device 400 that operates in accordance with a location policy and user device information. *See* Abstract. The location policy refers to a rule or other type of information referring to the operation of a mobile user device within proximity to a location device. A location device 1000 may evaluate user device information and transmit an appropriate location policy to a mobile user device 400. Also, the location device 1000 may simply determine whether or not a location policy will be applied based on the user device information. *See* paragraphs [0052]-[0059]. The mobile user device also operates in accordance with a device policy. Information about the device policy is received from the wireless communication device. The device policy is then compared with the location policy. If the location

policy is compatible with the device policy, then information is transmitted to arrange for the wireless communication device to communicate in accordance with the location policy and the device policy. *See* paragraphs [0105]-[0107].

However, there is nothing in Stern that discloses or teaches a **cipher apparatus** that receives information of the portable terminal, **obtains a secret code** for the locked state of the camera from a database, and **transmits enciphered data obtained from the secret code**. Nowhere does Stern teach or suggest that the portable terminal receives and deciphers enciphered data. Stern discloses a location device 1000 that receives user device information from a PDA indicating that the PDA is registered to a student. The location device 1000 compares the registration information of the PDA with the location policy and transmits information to the PDA indicating that the PDA is not allowed to wirelessly exchange information. *See* paragraph [0058].

Stern further discloses that the location device 1000 may also instruct a digital camera that no pictures are to be taken during a concert performance. The digital camera may then transmit an offer to provide payment of five dollars in exchange for permission to take ten pictures. The location device 1000 can then reject the offer, accepts the offer, or propose a counter-offer to the digital camera. *See* paragraph [0059]. The location device 1000 operates in accordance with a policy associated with a pre-defined set of rules for operation. *See* paragraph [0056]. Essentially, the mobile user device of Stern receives information from a location device 1000 comprising a location identifier (e.g., a concert hall or a school) and a location policy associated with the location (that is, a set of rules or other type of information that can be associated with the operations of the mobile user device).

However, there is nothing in Stern that discloses or teaches that the location device is a **cipher apparatus** that receives information of the mobile user device, **obtains a secret code** for the locked state of a camera from a database, and **transmits enciphered data obtained from the secret code**. Moreover, there is nothing in Stern that discloses or teaches that the mobile user device 400 of Stern receives and deciphers enciphered data. The mobile user device of Stern receives a location policy

from a location device. Nowhere does Stern teach or suggest **comparing a secret code received from the cipher apparatus with one of the secret codes stored in the memory**. Furthermore, there is nothing in Stern that discloses or teaches that a camera is enabled to operate **when a secret code matches said one of the secret codes stored in the memory**.

To cure the deficiencies of Hunter and Stern, the Examiner relies on Menzel for teaching a mobile device and a base station that exchange public keys, which the Examiner alleges as reading on the secret code of the present application, by referencing col. 2, lines 7-19 and col. 2, lines 48-58. The Examiner further relies on Menzel for teaching a method of encrypting data using the exchanged public keys in subsequent communication, by referencing col. 2, lines 9-19 and col. 2, lines 51-58. According to the Examiner, it would have been obvious to one of ordinary skill in the art at the time the invention was made for a mobile device and a base station to exchange public keys and encrypt the data using the exchanged public keys in subsequent communication, since Menzel states at col. 3, lines 3-29 that encrypted communication provides for secure communication between the devices, thereby preventing unauthorized users from intervening in the exchange of information.

Menzel discloses a method for encrypting information for a radio transmission and for authentication of subscribers in a communication system. *See* col. 1, lines 9-12. The method of encryption of Menzel comprises encrypting subsequent information to be transmitted via the radio interface using one of the public keys received by the base station or the mobile station, and deciphering encrypted information received by the mobile station or the base station on the basis of a private key that is allocated to the transmitted public key in the mobile station or in the base station. *See* col. 2, lines 4-19. Menzel further discloses that the public keys received by the base station or mobile station is employed for the encryption of information to be subsequently transmitted via the radio interface, and the encrypted information received by the mobile station or the base station can be deciphered on the basis of a private key that is allocated in the mobile station or in the base station that the public key was transmitted. The public keys in Menzel are transmitted in alternation

between the base station and mobile station that can be used in parallel by a plurality of subscribers. *See* col. 5, lines 27-46.

However, there is nothing in Menzel that discloses or teaches that the public key transmitted by the mobile station to the base station and the public key employed by the base station comprise a secret code for the locked state of a camera from a database. There is nothing in Menzel that teaches that the private keys employed by the mobile station or base station are obtained from a secret code for the locked state of a camera from a database. Information of Menzel is encrypted for radio transmission. *See* col. 2, lines 20-22. Transmitters in the mobile station and base station mutually send public keys via a radio interface. Controllers in the mobile station and the base station encrypt the information sent via the radio interface upon employment of public keys received by the base station or the mobile station. Accordingly, public keys and private keys are mutually sent to each other. Moreover, the base station or mobile station of Menzel does not transmit public keys that correspond to a secret code for a locked state of a camera. Furthermore, the private keys of Menzel do not comprise enciphered data obtained from a secret code.

Nowhere does Menzel teach or suggest comparing a secret code received from a cipher apparatus with one of the secret codes stored in a memory and enabling a camera to operate when the secret code matches said one of the secret codes stored in memory.

Menzel discloses a mobile station that sends a first public key via a radio interface in parallel for all subscribers active at it and makes note of an appertaining private key that is deposited in the memory or the controller. The base station employs the received public key for the encryption of information to be subsequently sent via the radio interface. The deciphering of the information sent by the base station is thus only possible for the entity that knows the appertaining private key, i.e., the mobile station with the private key. The base station in turn sends a public key in reply of the base station and makes note of the appertaining private key. The memory or the controller of the base station stores the private key. Information subsequently sent by the mobile station to the base station, which is encrypted upon employment of the public key, can only in turn be deciphered by the base station or its controller.

There is nothing in Menzel that discloses or teaches comparing a public key with a public key stored in the memory. Nowhere does Menzel teach or suggest enabling a camera to operate when the public key matches one of the public keys stored in memory. Also, there is nothing in Menzel that discloses or teaches that enciphered data is transmitted to a portable terminal and subsequently, the portable terminal deciphers the enciphered data. The public keys and private keys of Menzel are mutually sent between the base station and mobile station. Accordingly, Menzel does not disclose or teach a method for comparing a secret code received from the cipher apparatus with one of the secret codes stored in the memory and enabling a camera to operate when the secret code matches said one of the secret codes stored in memory.

Regarding the Examiner's reasoning for combining Hunter, Stern and Menzel, there is nothing in the references that discloses or teaches a cipher apparatus that receives information of the portable terminal, obtain a secret code **for the locked state of the camera** from a database, the cipher apparatus transmitting enciphered data **obtained from the secret code, comparing the secret code received from the cipher apparatus with one of the secret codes stored in the memory**, and enabling the camera to operate **when the secret code matches said one of the secret codes stored in the memory**. Accordingly, the combination of the references does not result in the claimed invention.

In view of the above arguments, independent claim 8 would not have been obvious from any reasonable combination of Hunter, Stern and Menzel at least for reasons noted above.

Accordingly, Applicants' independent claim 8, as well as dependent claims 9-11 (which incorporate, by reference, all of the features of their respective base claim) are patentable over Hunter, Stern and Menzel at least for these reasons. Applicants therefore respectfully submit that Hunter, Stern and Menzel cited above by the Examiner fail to teach or suggest all of the limitations of independent claim 8 as set forth in embodiments of the present invention.

For at least these reasons, the rejections of independent claim 8, as well as dependent claims 9-11, which incorporates all of the limitations of base claims 8, should be withdrawn based on the above arguments.

#### **Allowable Subject Matter**

Applicants thank the Examiner for the allowance of claims 3-7. After the Examiner's consideration of the arguments presented herein, claims 8-11 are also believed to be in condition for allowance.

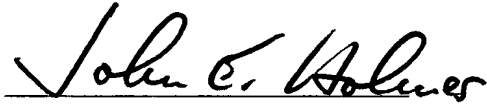


### Conclusion

Reconsideration of the above-identified application and allowance of claims 3-11 are respectfully requested.

In view of the above, it is believed that the application is in condition for allowance and notice to this effect is respectfully requested. Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the telephone number indicated below.

Respectfully submitted,



John E. Holmes  
Attorney for Applicants  
Reg. No. 29,392

Roylance, Abrams, Berdo & Goodman, L.L.P.  
1300 19<sup>th</sup> Street, N.W., Suite 600  
Washington, D.C. 20036  
(202) 659-9076

Dated: July 7, 2008